

# Behavior Patterns Before and After infection with a File-Infecter virus

Pre Infection

Operating System Functions Called

Create New Window  
Load resources  
Wait for user input  
Load Document  
Wait for User input  
Check file size  
Write to Document  
Close File

0000 1000 1000 0110 1001 0001 0101 0011 0010 1101 0101 0100 0101 1101 0101 1111

Post Infection

Operating System Functions Called

Modify INT21 address  
INT21 points at CS  
Search for first EXE  
Move to End-of-file  
Check size of file  
if: Larger than 10K  
Write to File  
Search for next EXE

User Input

0010 1100 1010 1110 1001 0101 0101 0011 0010 1101 0101 0101 0101 1101 0100 1011

FIG. 1

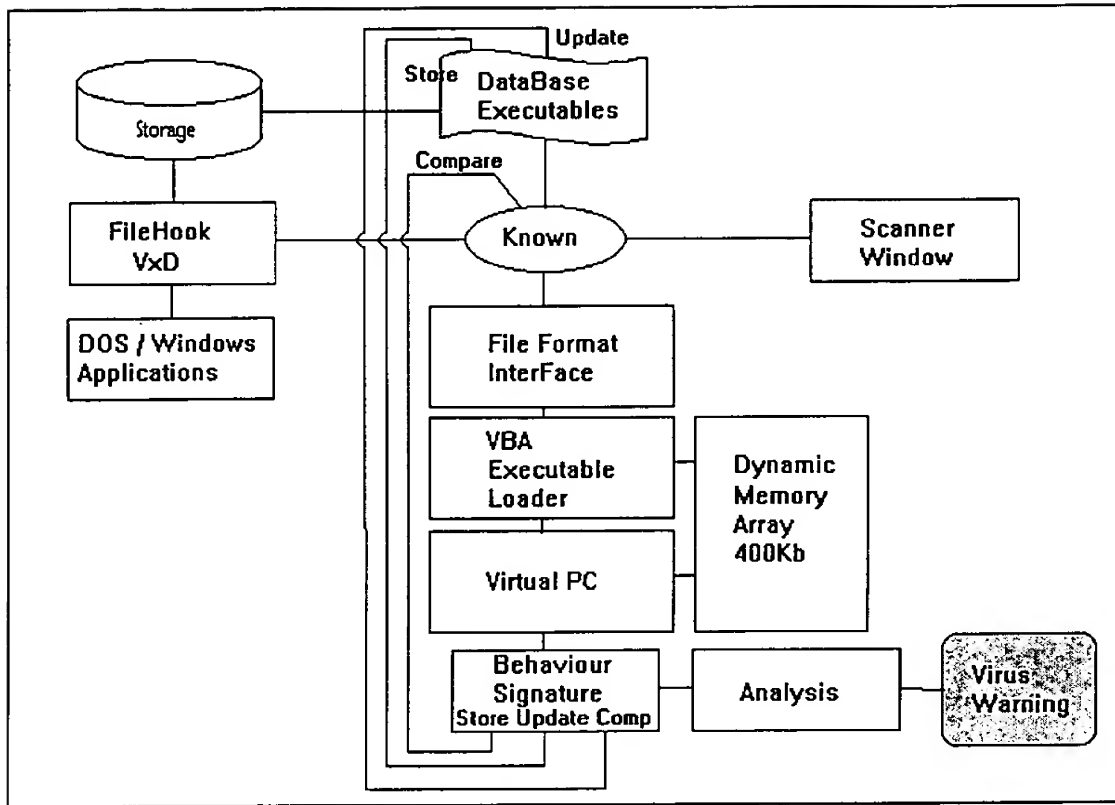


FIG. 2

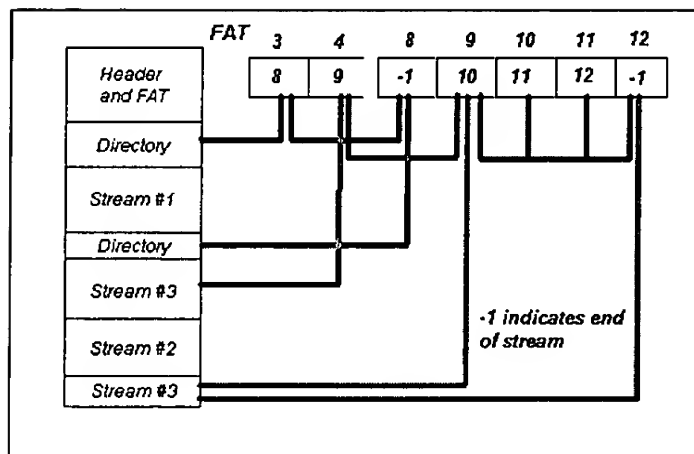


FIG. 3

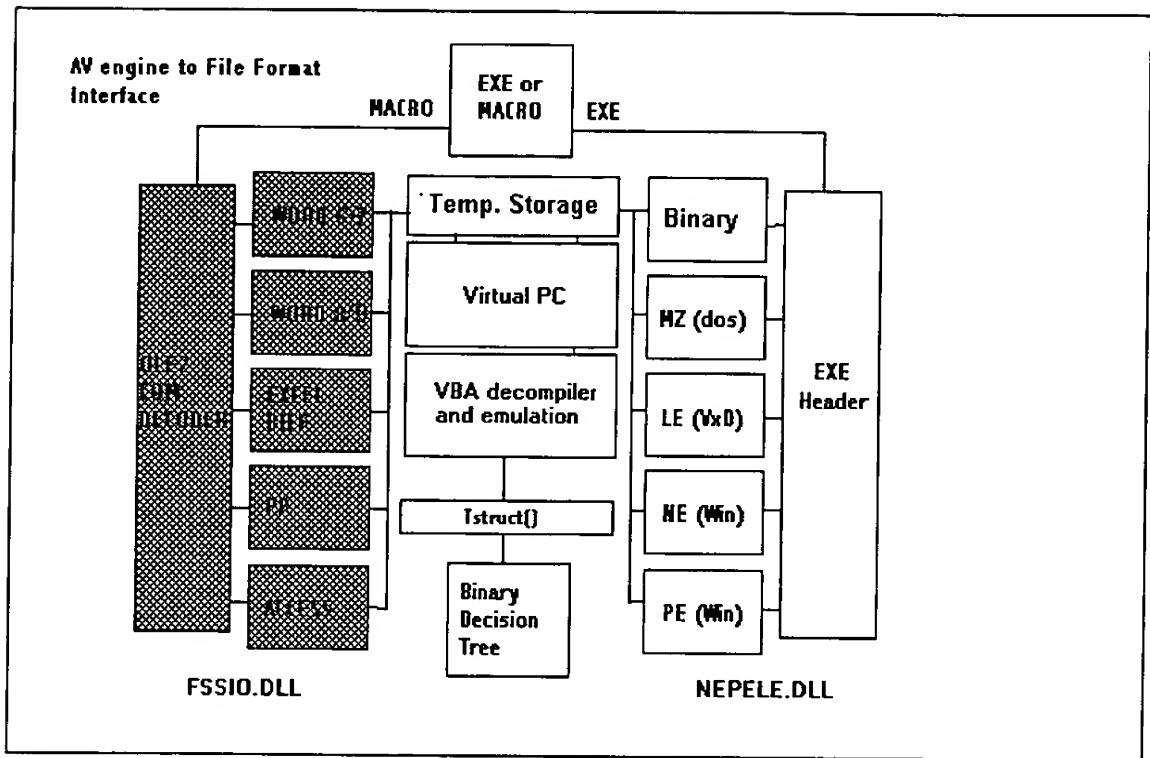


FIG. 4

# V80X86

## MEMORY MAPS FOR BINARY COM AND EXE FILES

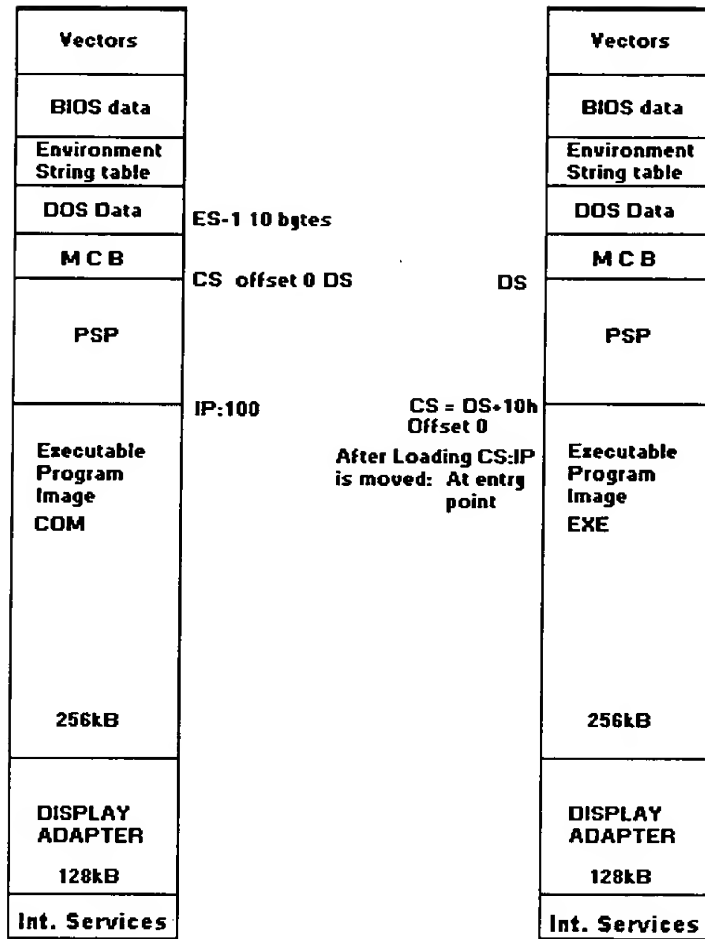


FIG. 5

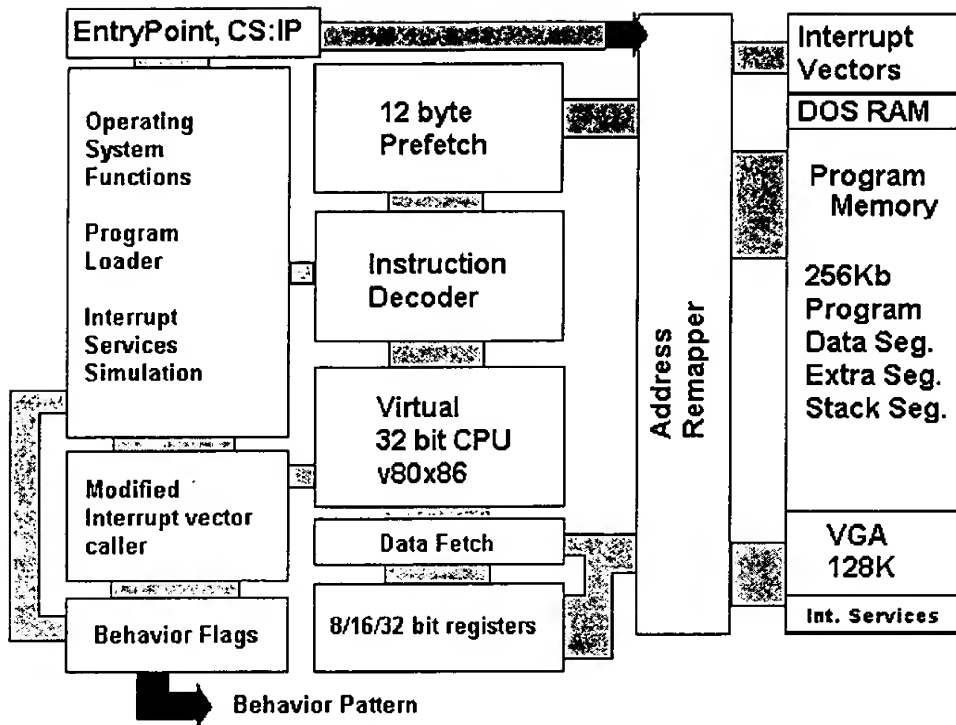


FIG. 6